DISN Video Services (DVS) Customer Connection Approvals

DVS Information Assurance Support

July 2010

Agenda

- Purpose
- Customer Configurations
- Connection Approvals

Purpose

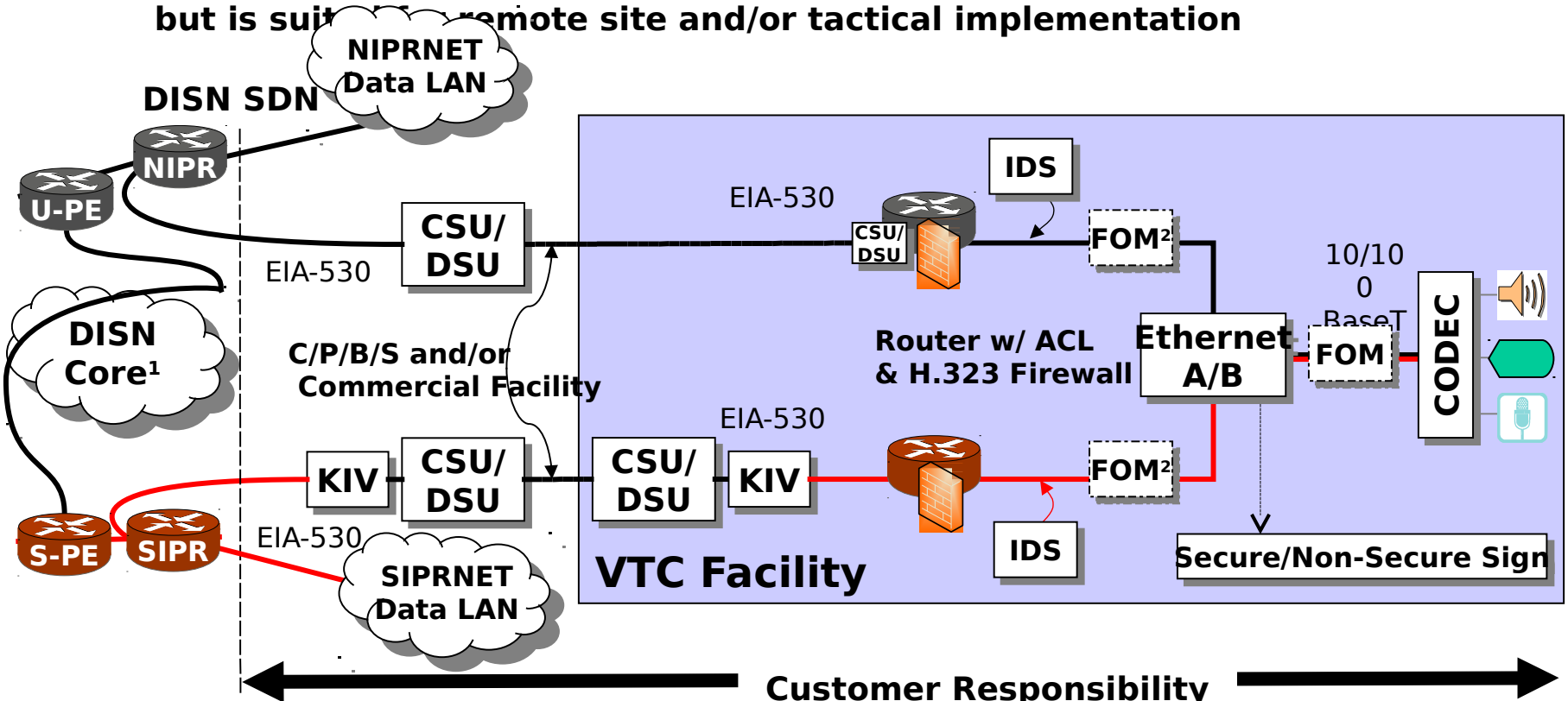
- **Present approved customer configurations and IA controls**
  - **Video IP Network**
  - **Dial-up Connection**
  - **Hybrid Connection**
  - **Periods Processing**
  - **Non Open Storage VTC Facility**
  - **Available Products**
- **Identify required connection approvals to access DVS**
  - **Non-DoD Connection Validation Letter**
  - **Order transmission paths**
  - **DSN Certification**
  - **VTC System Certification and Accreditation**
  - **PPSM Registration**
  - **SIPRNet, NIPRNet, DSN, and DVS Authority to Connect**

Customer Configurations

- **Video IP Network Minimum Requirements**
  - **Dedicated video network separate from the data network, e.g. video VLAN**
  - **Network protection consisting of Router with ACL, H.323 aware Firewall or H.460 tunneling, and Intrusion Detection System (IDS)**
  - **Approved Ethernet A/B switch for switching between Classified and Unclassified networks**
  - **External indicators of secure/non-secure connection status**
  - **Fiber Optic Modem (FOM)/Transceiver powered-off in the path that is not used**
  - **Periods processing procedures to remove residual information when switching devices between classification levels**
  - **H.323 CODEC**

Customer Configurations

- **Option 1 – Classified/Unclassified Single Facility Direct IP Connection**
  - **Originally designed to quickly transition dedicated DVS-G sites to IP Video, but is suit[illegible]emote site and/or tactical implementation**



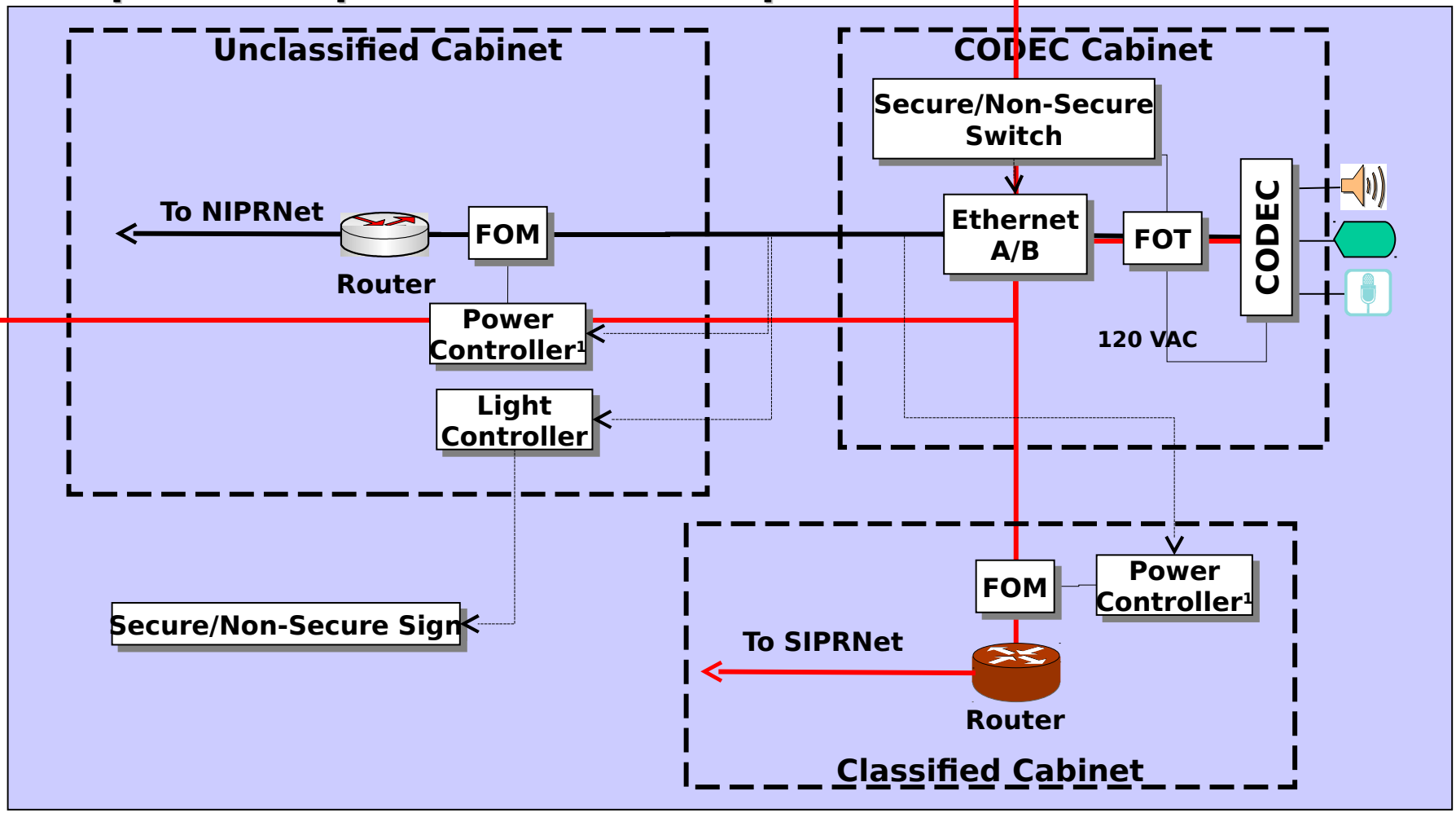
1 Or Customer WAN with QoS and connection to DISN

2 Fiber Optic Modem (FOM)/Transceiver powered-off in the path that is not used

Mission First | GIG Combat Support | People Always

Customer Configurations

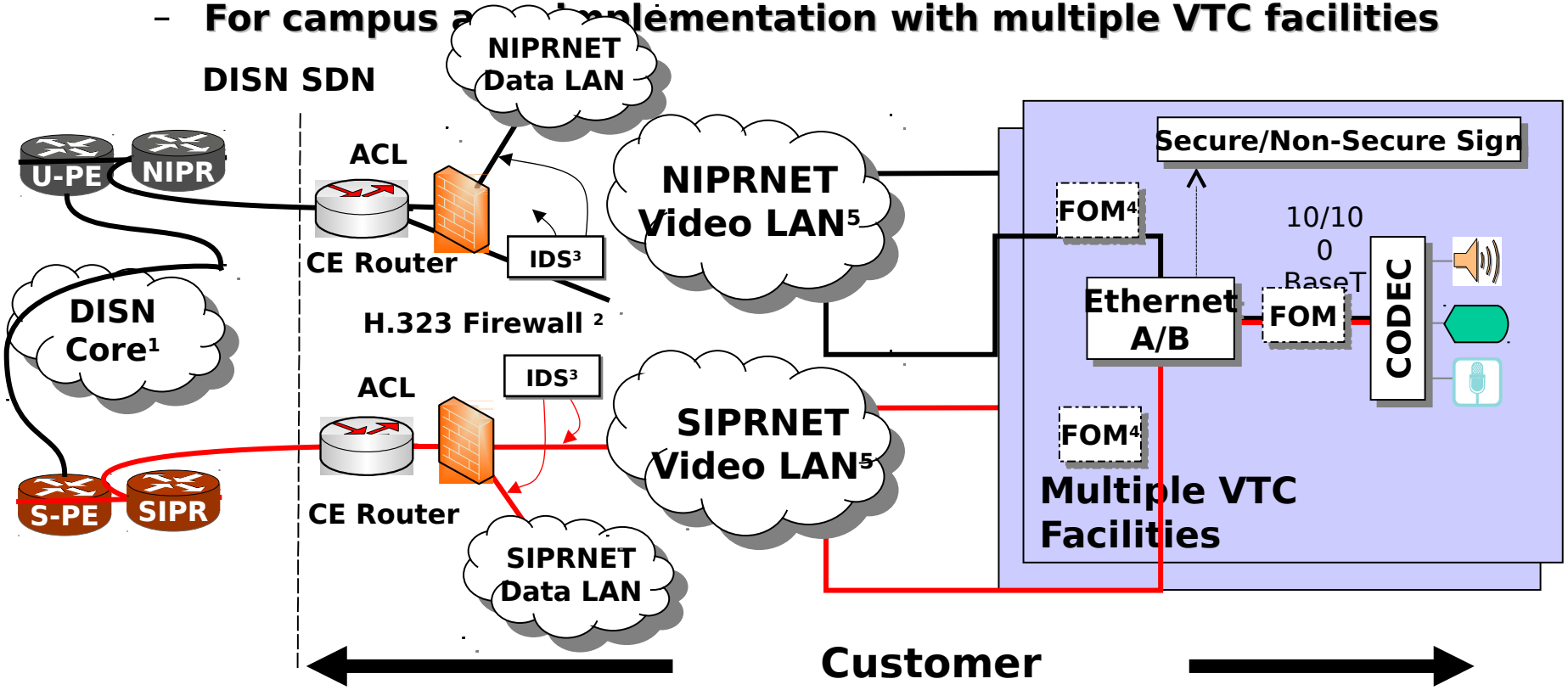
- **Option 1 Implementation Example**



1 Powers off Fiber Optic Modem (FOM) in the path that is not used

Customer Configurations

- **Option 2 – Classified/Unclassified Multiple VTC Facilities Video IP Network**
  - **For campus a[illegible]mplementation with multiple VTC facilities**



1 Or Customer WAN with QoS and connection to DIS

2 The same Firewall could be used for both video and data provided it has the required performance and functionality, i.e. H.323 aware

3 IDS to monitor each network segment IAW the Network STIG

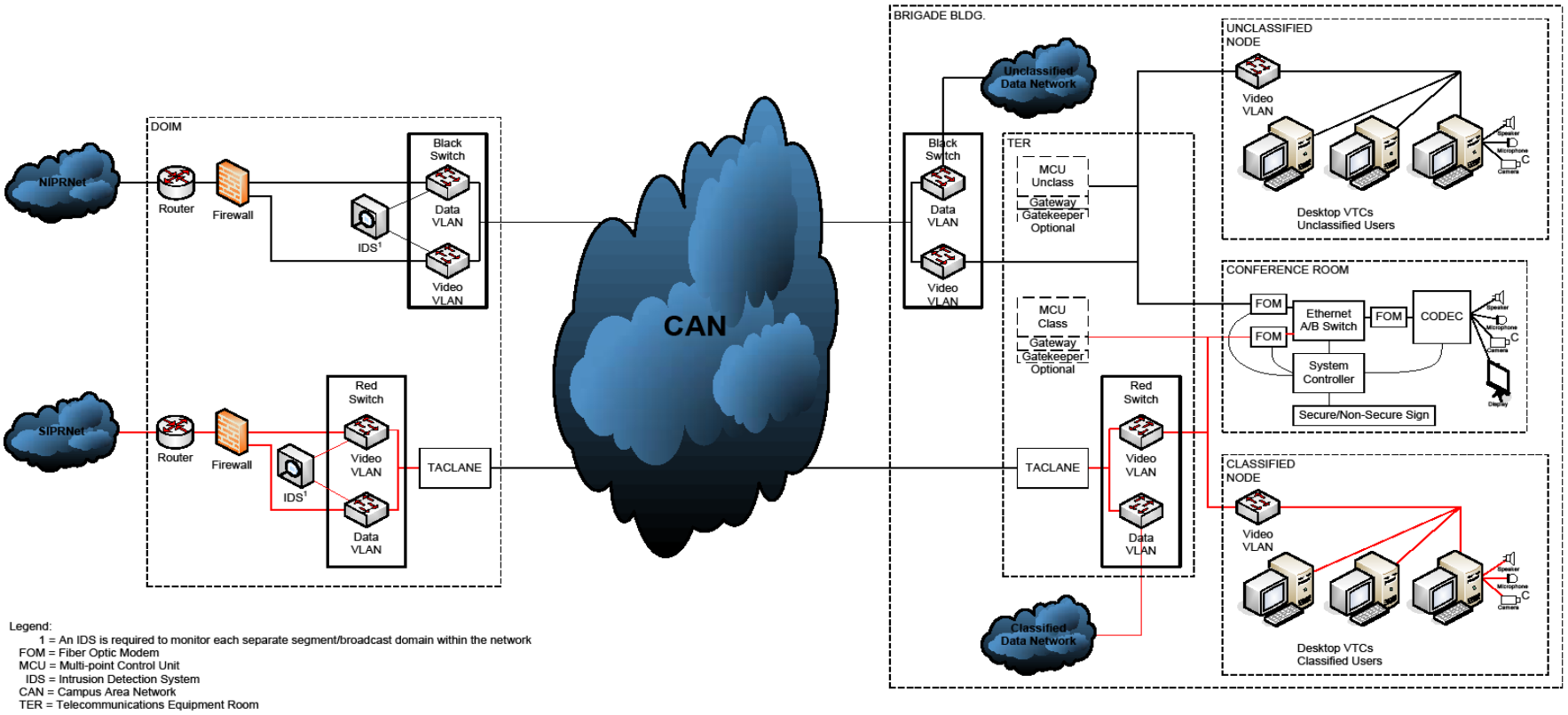
[illegible])/Transceiver powered-off in [illegible]

5 Separate VLAN or physical network from the data LAN

Mission First | GIG Combat Support | People Always

Customer Configurations

- **Option 2 Implementation Example**

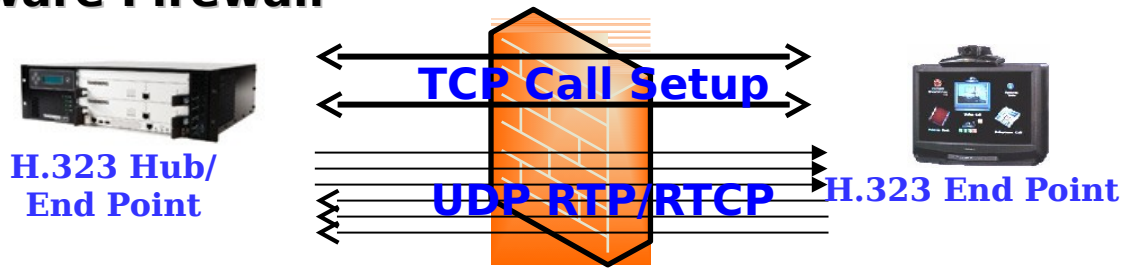


Legend:
1 = An IDS is required to monitor each separate segment/broadcast domain within the network
FOM = Fiber Optic Modem
MCU = Multi-point Control Unit
IDS = Intrusion Detection System
CAN = Campus Area Network
TER = Telecommunications Equipment Room

Note: MCUs, Gateways, and Gatekepers are optional customer video infrastructure components implemented on a separate network segment/VLAN than the Conference Room and Desktop VTCs.

Customer Configurations

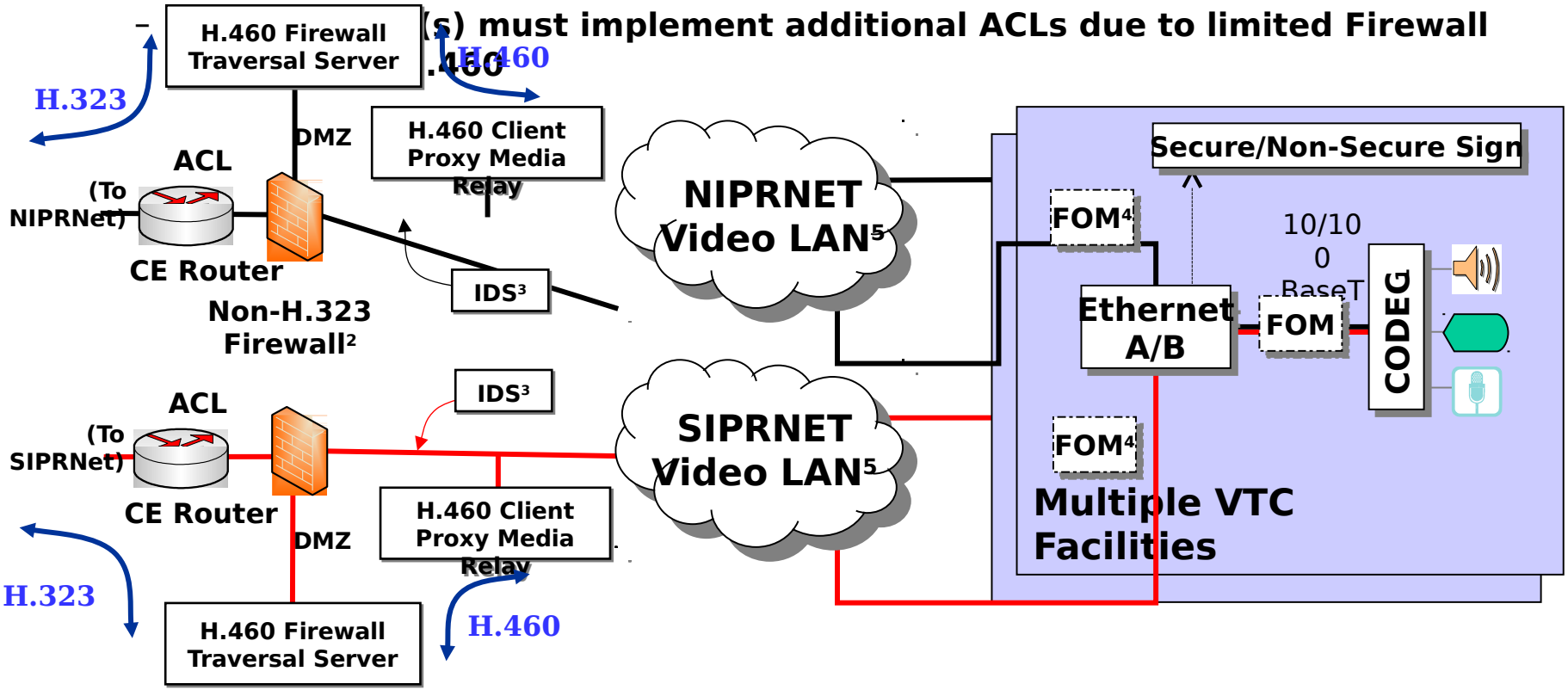
- **H.323 Aware Firewall**



  - **Understands the H.323 protocol and dynamically open the ports needed by the video session and closes them when the session is over**
  - **H.323 Ports**
    - **1718 UDP – H.225.0 Gatekeeper Discovery**
    - **1719 UDP – H.225.0 Gatekeeper RAS**
    - **1720 TCP – H.225.0 Call Signaling**
    - **1025-65535 Dynamic TCP – H.245 Media Control**
    - **Even-numbered ports above 1024 UDP – RTP (Media Stream)**
    - **Next corresponding odd-numbered ports above 1024 UDP – RTCP (Control Information)**
  - **Gatekeeper Name Resolution**
    - **53 TCP/UDP – DNS Lookup**

Customer Configurations

- **H.460 Firewall Traversal**
  - For customers doing video now and cannot upgrade to an H.323 aware Firewall
  - (s) must implement additional ACLs due to limited Firewall



1 Non-H.460 aware CODECs need to go via the H.460 Client Proxy Media Relay to traverse the Firewall

2 The same Firewall could be used for both video and data provided it has the required performance

3 IDS to monitor each network segment IAW the Network STIG

4 Fiber Optic Modem (FOM)/Transceiver powered-off in the path that is not used

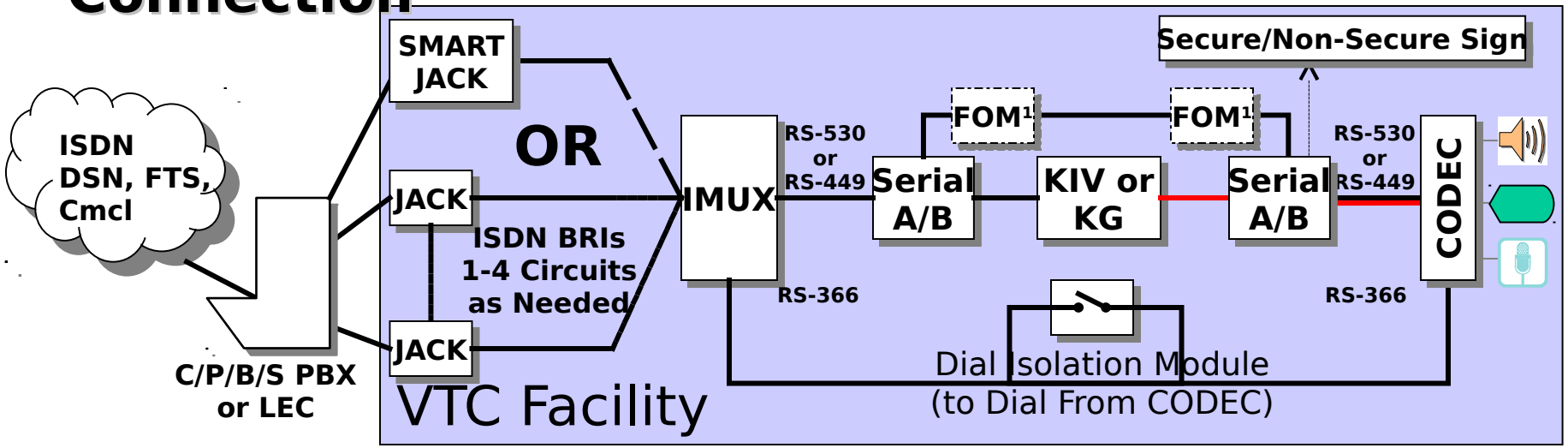
5 Separate VLAN or physical network from the data LAN

Customer Configurations

- **Dial-up Connection Minimum Requirements**
  - **DSN Certified hardware and/or software for sending and receiving voice, data or video signals, e.g. IMUX, CODEC**
  - **Tempest 2/95-A compliant Serial A/B switches and/or Fiber Optic Modems for Red/Black isolation**
  - **Dial isolator to dial from the CODEC**
  - **Type 1 encryption for classified connection**
  - **External indicators of secure/non-secure status**
  - **Periods processing procedures to remove residual information when switching devices between classification levels**
  - **H.320 CODEC**

Customer Configurations

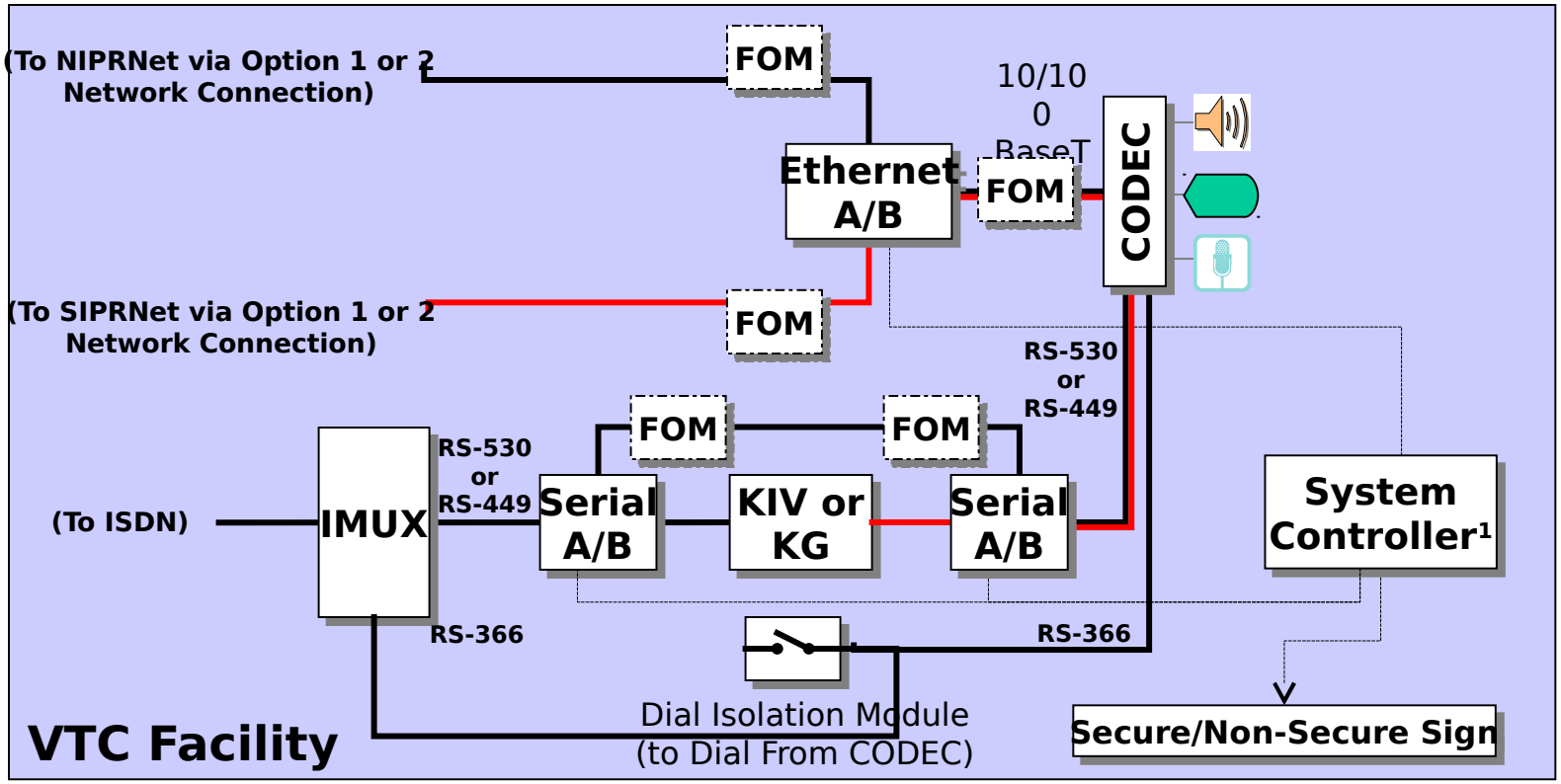
- **Option 3 – Classified/Unclassified Dial-up Connection**



1 Fiber Optic Modem (FOM)/Transceiver powered-off in the path that is not used in lieu of Red/Black isolation within the Serial A/B switch

Customer Configurations

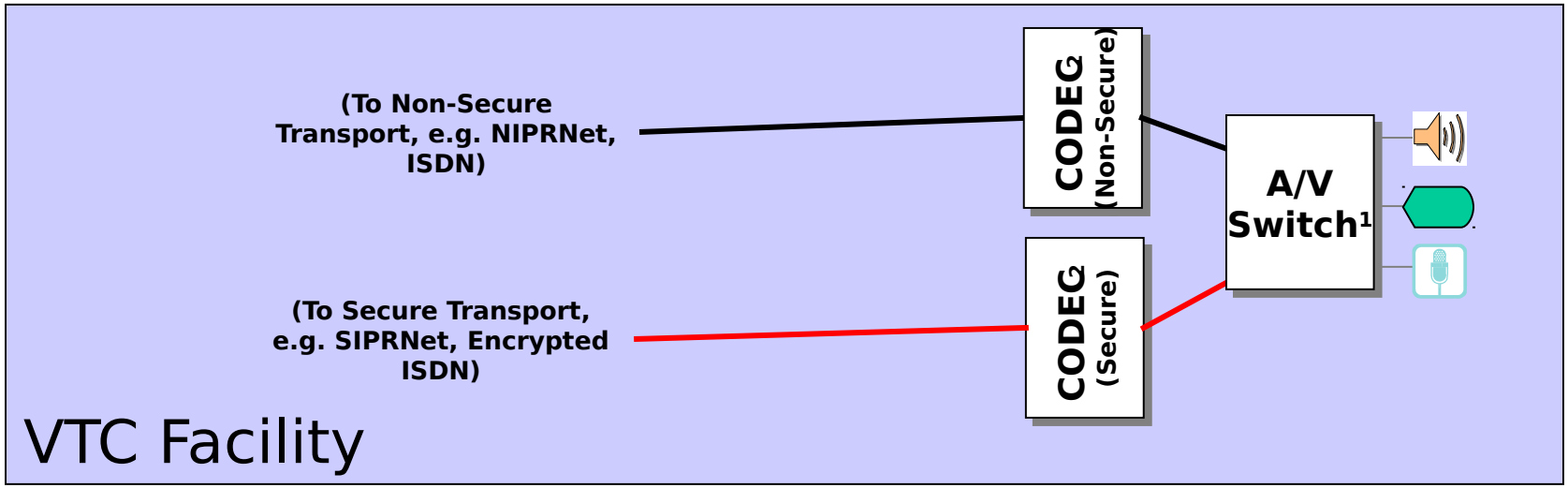
- **Option 4 - Classified/Unclassified Hybrid IP and Dial-up Connections**



1 A/B Switches centrally controlled to ensure that both IP and Dial-up connections are at the same classification level

Customer Configurations

- **Dual CODECs solution in conjunction with approved options**



1 Shared peripherals, e.g. speaker, display, microphone, should be connected via an approved peripheral sharing device/switch

2 CODEC that is not active must be powered-off

Customer Configurations

- **Periods Processing for Single CODEC**
  - **Required when switching between classification levels and between conferences to clear residual information**
  - **Data Classification**
    - **On a classified CODEC: audio/video media stream is classified information; other information such as IP Addresses, address book entries, call logs and call data records are sensitive information and could be classified when sufficient information are compiled**
  - **Assumptions**
    - **Audio/video media stream is stored/processed on volatile memory during a call**
    - **Environment 1 – CODEC does not store sensitive information on non-volatile memory, e.g. directory services is disabled and not used to store address book entries, call logs and call data records are disabled, etc.**
    - **Environment 2 - CODEC store sensitive information on non-volatile memory, e.g. directory services are used to store address book entries, call logs or call data records cannot be disabled, etc.**

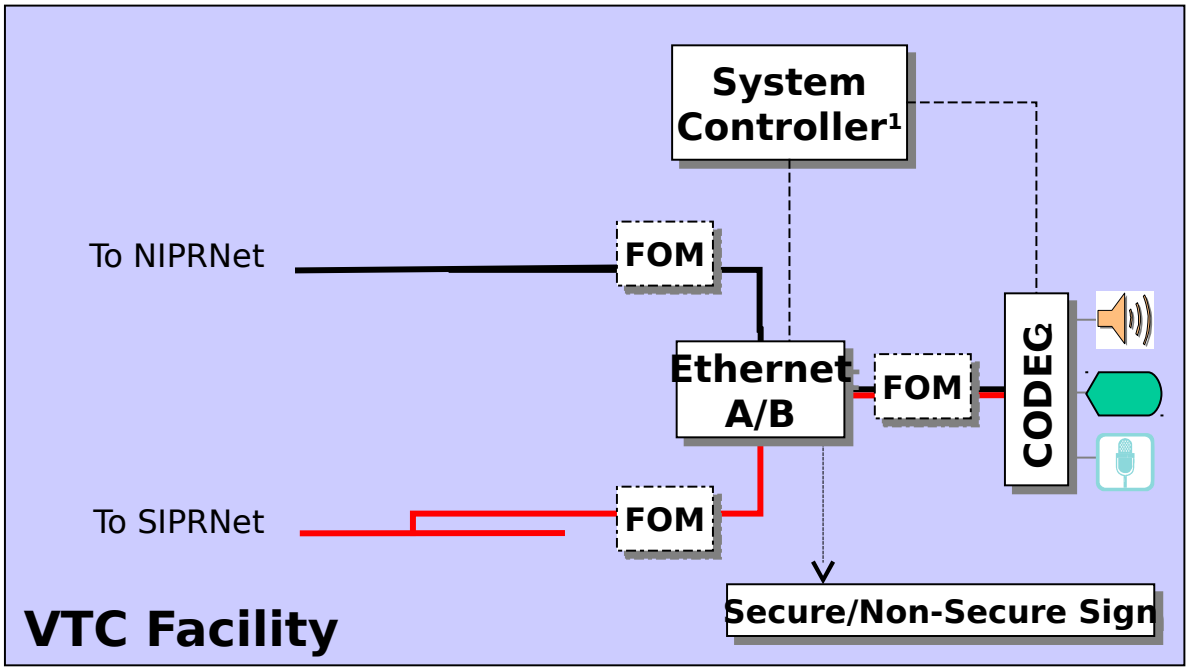
Customer Configurations

- **Periods Processing for Single CODEC (cont'd)**
  - **Procedures**
    - **Disconnect CODEC from the network to go to transition state**
    - **REMOVE RESIDUAL INFORMATION**
      - **For environment 1, power cycle the CODEC to sanitize residual information on volatile memory**
      - **For environment 2, sanitize residual information stored on volatile and non-volatile memory, then reload/reconfigure required information**

        Note:
        - **Coordinate with vendor/solutions provider and Certifier to ensure that all residual information are sanitized based on equipment configuration**
        - **CODECs with persistent memory, e.g. compact flash, are treated as storage media and should be removable or not used for periods processing**
      - **Remove storage media with different classification level/no-need-to-know information on equipments; equipments with non-removable storage media are not allowed for periods processing**
    - **Verify that there is NO RESIDUAL INFORMATION on equipments and configure for the new network**

Customer Configurations

- **Periods Processing for Single CODEC (cont'd)**
  - **Using System Controller**



1 System Controller should only provide out of band control, i.e. switch Ethernet A/B, reboot CODEC; otherwise, it must only be connected to the CODEC during transition state, i.e. not connected to either NIPRNet or SIPRNet, and disconnected at all other times using an approved RED/BLACK disconnect

2 IP parameters on the CODEC could be automatically obtained from the network DHCP server during restart, eliminating the need to store configuration parameters on the System Controller

Customer Configurations

- **Non Open Storage VTC Facility**
  - **Lock boxes for SIPRNet wall ports (based on risk analysis of wall port access; enabling port security on the network switch could be an alternate and/or additional mitigation)**
    - **Model No. KL-102 at** http://www.hamiltonproductsgroup.com/GSA/Key.html
    - **Model No. GL-1259 at** http://www.diebold.com/dnpssec/government/solutions/containers_safes_storage/control_containers.htm
  - **Information Processing System (IPS) container for classified equipments, e.g. KIV/KG with crypto key, classified Router, etc.**
    - https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_nfesc_pp/locks/gsa_cont_main/gsacont_ips
  - **Removing crypto key and storing on GSA approved container**

    Note: This approach present some issues such as dealing with network alarms, crypto key update, and Router maintenance when the crypto key is removed
  - **Additional information for secure storage from the DoD Lock Program**
    - https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_nfesc_pp/locks

Customer Configurations

- **Available Products**

Type	Manufacturer	Comments
Router w/ ACL & H.323 Firewall[1]	Various	Approved products listed under Technology Type – Firewall at http://niap-ccevs.org/cc-scheme/vpl/
IDS[1]	Various	Approved products listed under Technology Type – IDS/IPS at http://niap-ccevs.org/cc-scheme/vpl/

1 Example products are the Cisco ASA 5500 Series Adaptive Security Appliances/Firewalls, Cisco 4200 Series IDS Sensors, and the integrated Cisco 1841 Router with IOS Firewall and AIM IDS Sensor. For Cisco 1841, Register at https://www.wwt.com/portalWeb/userSelfReg/begin.do, Partner Registration Code DVSII0708, then purchase at https://www.wwt.com/portalWeb/appmanager/maclogin/wwt

Customer Configurations

- **Available Products**

Type	Manufacturer	Comments
H.460 Firewall Traversal Server and Client Proxy Media Relay	Various, examples are: Radvision SCOPIA™ PathFinder™ Firewall Traversal (http://www.radvision.com/Products/Infrastructure/Firewall-Traversal/SCOPIA-PathFinder/) Polycom Video Border Proxy (http://www.polycom.com/products/telepresence_video/security_remote_access/index.html) Tandberg Expressway Solution (http://www.tandberg.com/video-firewall-traversal.jsp)	NIAP validation is required on devices performing primary ACL function for access to video resources on the protected network.

Customer Configurations

- **Available Products**

Type	Manufacturer	Comments
Power Controller	Various, example is: AMX PC1 (http://www.amx.com/products/PC1.asp)	Required to turn power on/off on the FOM/Transceiver
Fiber Optic Modem/ Transceivers	Various, examples are: Trendnet TFC-110 (http://www.trendnet.com/products/products.asp?cat=22) Canary CFT-2061 (http://www.canarycom.com/products/products_frameset.htm)	
Ethernet A/B	Market Central, Inc SecureSwitch (http://www.secureswitch.com/SecureSwitch.htm)	http://niap-ccevs.org/cc%2Dscheme/st/?vid=1030&maint=156
Ethernet A/B with System	Various	Recommended switches listed at http://disa.dtic.mil/disnvtc/red_black_peripherals.x

Customer Configurations

- **Available Products**

Type	Manufacturer Model Number Estimated Cost	Comments
Serial A/B	Various	Recommended switches listed at http://disa.dtic.mil/disnvtc/red_black_peripherals.xls
A/V Switch for 2 Codec Configuration	CIS Secure Computing DTD-DCS-AVS (http://www.cissecure.com/)	Added Red/Black isolation within the A/V Switch and power-off inactive CODEC
Peripheral Sharing Devices, e.g. KVM	Various	http://iase.disa.mil/stigs/downloads/pdf/unclassified_span_v1r2_stig_20100727.pdf
DSN Certified Components, i.e. H.320	Various	https://aplits.disa.mil/apl.jsp

Customer Configuration Checklist

Configuration Requirements	Option 1 Single CODEC IP Connection	Option 2 Multiple VTC Facilities Video IP Network	Option 3 Dial-up Connection
Router ACL, Firewall, and IDS protection IAW Network and Enclave STIGs (see list of applicable STIG checklists on pg. 28)	√	√	
Dedicated video LAN separate from the data network	√	√	
Router ACL and Firewall Policy only allow Video-over-IP protocol, i.e. H.323, connection to/from the CODEC – H.323 Content Based Access Control (CBAC) only allow traffic to/from the CODEC – Port security shutdown port on the switch if MAC Address other than the CODEC is detected	√ √	√ √	
H.460 Firewall Traversal Server placed on the DMZ, for sites that could not upgrade to an H.323 Firewall, with additional ACL implemented on other device(s)	√	√	
Approved Ethernet A/B switch for switching between Classified and Unclassified networks on single CODEC solution	√	√	
External indicators of secure/non-secure status	√	√	√

Customer Configuration Checklist

Configuration Requirements	Option 1 Single CODEC IP Connection	Option 2 Multiple VTC Facilities Video IP Network	Option 3 Dial-up Connection
System Controller containing sensitive or classified information to reconfigure the CODEC, e.g. IP Address and address book entries, must only be connected to the CODEC during transition state and disconnected at all other times using an approved RED/BLACK disconnect	√	√	
DSN Certified hardware and/or software designed to send and receive voice, data or video signals, e.g. IMUX, CODEC (https://aplits.disa.mil/apl.jsp)			√
Tempest 2/95-A compliant Serial A/B switches and/or Fiber Optic Modems for Red/Black isolation			√
Dial isolator for disconnecting dial-in line from the CODEC			√
Type 1 encryption for classified connection with established key management procedures	√	√	√

Customer Configuration Checklist

Configuration Requirements	Option 1 Single CODEC IP Connection	Option 2 Multiple VTC Facilities Video IP Network	Option 3 Dial-up Connection
Fiber Optic Modem (FOM)/Transceiver powered-off in the path that is not used (Not applicable for Option 3 if using a Tempest compliant Serial A/B switches)	√	√	√
Non-secure services disabled on the CODEC, e.g. http telnet, and ftp if IP interface is used	√	√	√
Periods processing procedures to remove residual information	√	√	√
Only allowed users can access the CODEC, including protecting access to the CODEC with password	√	√	√
Disable microphone and cover camera if auto answer is required on the CODEC	√	√	√
CODEC that is not active must be powered-off on dual CODECs solution	√	√	√
Facility authorized for secure VTC (see NSTISSAM TEMPEST /2-95A for RED/BLACK Installation Guidance, and DoD 5220.22-M National Industrial Security Program Operating Manual, Chapter 5 - Safeguarding Classified Information)	√	√	√

Customer Configuration Checklist

Configuration Requirements	Option 1 Single CODEC IP Connection	Option 2 Multiple VTC Facilities Video IP Network	Option 3 Dial-up Connection
Dual CODECs – Shared peripherals should be connected via an approved peripheral sharing device/switch – CODEC that is not active must be powered-off	√ √	√ √	√ √
On hybrid connections, A/B Switches should be centrally controlled to ensure that both IP and ISDN connections are at the same classification level	√	√	√
Non-Open Storage VTC Rooms – Lock boxes for SIPRNet wall ports based on facility risk of unauthorized access – Information Processing System (IPS) container for classified equipments, e.g. KIV/KG with crypto key, classified Router, etc. – Removing crypto key and storing on GSA approved container	√ √ √	√ √ √	 √ √

Customer Configuration Checklist

- **The following are the typical STIGs for a dial-up VTC Facility:**
  - **IA Control Checklist**
  - **Video Teleconference (VTC) Checklist**
  - **DoD Telecommunications & Defense Switched Network (DSN) Checklist**
- **The following are the typical STIGs for an IP VTC Facility:**
  - **IA Control Checklist**
  - **Video Teleconference (VTC) Checklist**
  - **Network Security Checklist – Firewall**
  - **Network Security Checklist – General Infrastructure Router**
  - **Network Security Checklist – Intrusion Detection System (IDS)**
  - **Network Security Checklist – Network Policy**
- **Security checklists are located at** http://iase.disa.mil/stigs/checklist/index.html

Connection Approvals

Non-DoD customers

- Complete and Submit the Non-DoD Connection Validation Letter; download at http://www.disa.mil/connect/library/files/val_nondod_request.doc
- DISN SM reviews proposed solution
- CC/S/A reviews proposed solution
- OASD(NII) reviews proposed mission and DISN solution

Order transmission paths

https://www.disadirect.disa.mil/products/ASP/welcome.ASP

- SIPRNet and NIPRNet
- DSN Switched Digital Service
- FTS-2001 ISDN
- Commercial ISDN

Connection Approvals

DSN Certification

Interoperability and Information Assurance testing of hardware and/or software designed to send and receive voice, data or video signals across a network that provides customer voice, data or video equipment access to the DSN or PSTN, e.g. ISDN CODECs/MCUs, IMUX:

- Complete test submittal
- Perform vendor pre-scheduling actions
- Verify technical sufficiency and issue tracking number
- Schedule product for IO and IA testing
- Conduct initial contact meeting
- Perform self-assessment evaluation
- Conduct Information Assurance (IA) testing
- Conduct Interoperability (IO) testing
- Conduct out brief meeting
- DSAWG validate IA certification
- JS validate IO certification
- Add equipment to the Approved Products List (APL) at https://aplits.disa.mil/apl.jsp
- Detailed process description at http://www.disa.mil/ucco/apl_submission.html

Connection Approvals

Video Teleconferencing (VTC) System Certification and Accreditation (C&A):

- Requires an Authority to Operate (ATO) from the DAA using DIACAP
- DoD C&A Policy and DIACAP reference are located at http://iase.disa.mil/diacap/
- C&A implementation is directed by the customer's DAA
- DISA has developed traceability of STIG test results to the 8500.2 IA controls/DIACAP Scorecard Matrix to facilitate VTC Facility accreditation
  - The Scorecard Matrix and instructions are posted at *http://www.disa.mil/disnvtc/scorecard.htm*
  - The Scorecard Matrix identifies how to validate applicable controls for your VTF, including those from the VTC STIG

Connection Approvals

Video Teleconferencing (VTC) System Certification and Accreditation (C&A):

- Army
  - DAA: Various (contact Army Account Manager with questions)
  - DAA Representative(s):
    - Sally Dixon, sally.dixon@us.army.mil, 703-602-7376/DSN 332
    - Gary Robison, gary.robison@us.army.mil, 703-602-7395/DSN 332
    - Group Email, IACORA@us.army.mil

- Air Force
  - DAA: General Senty
  - DAA Representative(s):
    - AF Network Operations Center/A5
    - Emily J. Darnall, Information Assurance Manager, CSC,
      emily.darnall.ctr@barksdale.af.mil,
      emily.darnall.ctr@barksdale.af.smil.mil, 318-456-7684/DSN 781

Connection Approvals

Video Teleconferencing (VTC) System Certification and Accreditation (C&A):

- Navy
  DAA: Richard Voter
  DAA Representative(s):
  Naval Network Warfare Command
  Terry Halvorsen, SES, terry.halvorsen@navy.mil, 757-417-6700
  Richard Voter, YA-3, richard.voter@navy.mil, 757-417-7911
  Robert Mawhinney, YC-3, robert.mawhinney@navy.mil, 757-417-7912
- USMC
  DAA: Ray Letteer, 703-693-3490
  DAA Representative(s):

Connection Approvals

Video Teleconferencing (VTC) System Certification and Accreditation (C&A):

- DISA

  DAA: Henry J. Sienkiewicz

  DAA Representative(s):

  Steve Garron, steve.garron.ctr@disa.mil, 703-681-2065

  Note: DISA-owned VTC Facility must be included in the DVS ATO; Michael Bendel, michael.bendel.ctr@disa.mil, 703-681-3553 is the point of contact for this process.

Connection Approvals

Register CODEC on Ports and Protocols Services Management (PPSM) for video-over-IP connection to SIPRNet and NIPRNet

- **PVP – Packet Video Protocol (75)**
  - 1718 TCP/UDP - Gatekeeper Discovery
  - 1719 TCP/UDP - Gatekeeper RAS
  - 1720 TCP/UDP - H.323 Call Setup
  - 1025-65535 Dynamic TCP - H.245 (Call Parameters)
  - 1025-65535 Dynamic UDP - RTP (Video Stream Data) and RTCP (Control Information)
- **TCP (6)/UDP (17) – 53 - DNS Lookup**
- **PPSM Boundaries are:**
  - 12 - Enclave to Enclave DMZ
  - 10 - Enclave DMZ to DOD Network
  - 09 - DOD Network to Enclave DMZ (for calls terminating at a DVS Hub)
  - 11 - Enclave DMZ to Enclave (for point-to-point calls)
- **PPSM registration is available online at https://pnp.cert.smil.mil**

Connection Approvals

Authority to Connect (ATC)

- **SIPRNet**
  - Complete applicable approval requirements starting on pg. 28
  - Customer/Sponsor registers the connection information
  - Customer/Sponsor submits Connection Approval package
  - CAO reviews CAP package and makes a connection decision
  - Detailed process description at http://www.disa.mil/connect/instructions/classified.html

Connection Approvals

Authority to Connect (ATC)

- **NIPRNet**
  - Complete applicable approval requirements starting on pg. 28
  - Customer/Sponsor registers the connection information
  - Customer/Sponsor submits Connection Approval package
  - CAO reviews CAP package and makes a connection decision
  - Detailed process description at http://www.disa.mil/connect/instructions/unclassified.html

Connection Approvals

Authority to Connect (ATC)

- **DSN**
  - Complete applicable approval requirements starting on pg. 28
  - Customer/Sponsor registers the connection information
  - Customer/Sponsor submits Connection Approval package
  - Complete ATC Submittal form
  - CAO reviews CAP package and makes a connection decision
  - Detailed process description at http://www.disa.mil/connect/instructions/unclassified.html

Connection Approvals

Authority to Connect (ATC)

- **DVS**
  - Complete applicable approval requirements starting on pg. 28
  - Complete Initial Registration with Business Development (BD)
  - Submit CAP Documents to COMSEC Manager
  - Business Development Will Review Site Information
  - Designate Primary Facilitator with the VOC
  - Complete JITC site profile & equipment/facility verification
  - Complete AT&T Validation
  - Detailed process description for classified connection at http://www.disa.mil/connect/instructions/classified.html
  - Detailed process description for unclassified connection at http://www.disa.mil/connect/instructions/unclassified.html

DEFENSE INFORMATION SYSTEMS AGENCY